New Jersey State Legislature
Office of Legislative Services
Office of the State Auditor

Department of the Treasury
Division of Taxation
Online Database Security

May 15, 2006 to June 15, 2007

Richard L. Fair
State Auditor
The Honorable Jon S. Corzine
Governor of New Jersey

The Honorable Richard J. Codey
President of the Senate

The Honorable Joseph J. Roberts, Jr.
Speaker of the General Assembly

Mr. Albert Porroni
Executive Director
Office of Legislative Services

Enclosed is our report on the audit of the Department of the Treasury, Division of Taxation, Online Database Security for the period of May 15, 2006 to June 15, 2007. If you would like a personal briefing, please call me at (609) 292-3700.

Stephen M. Fells
Assistant State Auditor
September 6, 2007
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>1</td>
</tr>
<tr>
<td>Objectives</td>
<td>1</td>
</tr>
<tr>
<td>Methodology</td>
<td>1</td>
</tr>
<tr>
<td>Conclusions</td>
<td>2</td>
</tr>
<tr>
<td>Findings and Recommendations</td>
<td></td>
</tr>
<tr>
<td>System Administration</td>
<td>3</td>
</tr>
<tr>
<td>GENTS Access</td>
<td>4</td>
</tr>
<tr>
<td>Database Administration</td>
<td>6</td>
</tr>
<tr>
<td>Field Auditor Laptops</td>
<td>6</td>
</tr>
<tr>
<td>Documentation</td>
<td>7</td>
</tr>
<tr>
<td>Physical Access</td>
<td>8</td>
</tr>
<tr>
<td>Auditee Response</td>
<td>9</td>
</tr>
</tbody>
</table>
Department of the Treasury  
Division of Taxation  
Online Database Security

Scope

We assessed the adequacy of selected controls, policies and procedures over data security for the Department of the Treasury, Division of Taxation online databases as they relate to online tax applications for the period May 15, 2006 to June 15, 2007 excluding the division's data warehouse. We also evaluated the security controls over the Office of Information Technology (OIT) servers and databases that process and store the data captured. Our audit evaluated selected controls in place as follows:

- Business continuity plans in the event of processing interruptions.
- Protection of state resources from unauthorized access, use, and alteration.
- Change control process.
- Physical and logical security in place to protect the state's IT infrastructure.

Objectives

The objectives of our audit were to determine the adequacy of controls over the Division of Taxation's online databases to minimize the risk of unauthorized physical or logical access, to provide for business continuity, and to ensure changes are properly implemented and documented.

This audit was conducted pursuant to the State Auditor's responsibilities as set forth in Article VII, Section I, Paragraph 6 of the State Constitution and Title 52 of the New Jersey Statutes.

Methodology

Our audit was conducted in accordance with Governmental Auditing Standards issued by the Comptroller General of the United States. Additional guidance for the conduct of the audit was provided by the Open Source Security Testing
Methodology Manual issued by the Institute for Security and Open Methodologies, benchmarks issued by the Center for Internet Security, and Control Objectives for Information and Related Technology (COBIT) issued by the IT Governance Institute.

In preparation for our testing, we studied legislation, procedural guidelines and flow charts, and industry and governmental standards for computer security and operation. Provisions that we considered significant were documented and compliance with those requirements was verified by interview of key personnel, observation and access of network infrastructure, and through other tests we considered necessary.

A nonstatistical sampling approach was used. Our samples were designed to provide conclusions about internal control attributes. Sample items were selected judgmentally.

**Conclusions**

Division of Taxation and OIT management have recognized the importance of security over their databases and the information they contain. We found controls in place and functioning to minimize the risk of unauthorized physical or logical access, to provide for business continuity, and to ensure changes are properly implemented and documented. In making these determinations we noted certain control weaknesses meriting management’s attention.
System Administration

Solaris administration can be more effective with additional resources.

A review of user and file system security was performed to determine that the controls in place are sufficient to protect the servers from unauthorized access or attack. We tested the controls for seven servers. Four servers ran Unix and three ran Windows. Four of the servers are accessible from the Internet. The controls in place are adequate to currently protect the servers; however, policies should be adopted and additional resources should be devoted for the continued maintenance of those controls.

The Office of Information Technology (OIT) has several draft policies that address how security administration of operating systems, databases, and application access controls; security compliance monitoring; and security vulnerability management are to be applied to the organization. These policies have yet to be implemented. The result is that some matters are handled promptly while other issues are not addressed, including the need for a more rigid patch maintenance program, security monitoring, and vulnerability mitigation. We noted that there are only three Solaris administrators, one who is new to the OIT organization, to administer the approximately 130 Sun Unix servers currently in use at OIT. As a result, certain weaknesses existed. We brought them to management’s attention and they were corrected prior to the completion of our fieldwork.

Industry best security practices call for formal written policies and procedures to be in place and functioning to provide standards by which all servers could be measurably configured. The lack of written policies and procedures and periodic review of files, directories and security configurations, may result in the unauthorized access to or the compromise of confidential data without detection by employees in the performance of their normal duties.
Recommendation

We recommend that OIT management provide adequate resources to effectively administer the servers, finalize and implement draft policies to provide measurable standards for effectively mitigating potential security risks, and periodically review files, directories and security configurations to protect against unauthorized access or compromise.

GENTS Access

In a previous report dated December 12, 2002, we determined that access to the Generic Tax System (GENTS) was too widespread. Since that time the department has made an attempt to refine access from a top-down perspective. However, there has been no systematic review of existing job functions and GENTS roles. The current practice of modeling access levels after another employee is inappropriate. Our analysis found that 897 of 1900 (47%) users with the ability to perform some function in GENTS did not create a transaction to a taxpayer’s account during the period January to August 2006. In addition to these 897 users, there are 366 users with inquiry-only access to GENTS. Though it is understood that all users of GENTS do not make entries that affect taxpayers’ accounts, it appears many users have the unneeded ability to access and perform functions in GENTS. Standards indicate that access privileges should be limited to those required by a user and that management should review users’ access rights at regular intervals. Failure to properly limit access increases the risk of destruction or inappropriate disclosure of data.

Recommendation

We recommend that the division initiate a comprehensive review of GENTS access statewide. It should include reviewing access needs and roles with the users of the system from the bottom up, reviewing existing profiles in
Controls do not prevent GENTS users from making changes to their own tax accounts.

GENTS for relevance, and creating or adjusting roles in GENTS as necessary. In addition, access for each employee should be reviewed to determine if it is appropriate and necessary in this revised structure.

Currently, there is no control in place to prevent GENTS users with the proper access from making changes to their own tax accounts. The division's Standard Operating Procedure document states that "under no circumstances shall any employee personally make any adjustment or alteration to his or her own Division of Taxation account or record". Adjustments that need to be made are done so by a Division Employee Resolution Officer (DERO) after a written request is made and approved by the employee's immediate supervisor and appropriate section chief. Though the policy and threat of disciplinary action is an effective deterrent to prevent most users from adjusting their own accounts, our analysis of the transactions made to taxpayer accounts from January to July 2006 uncovered an instance where an employee made an adjustment to their own account. Management has already taken the appropriate disciplinary steps against this employee after we notified them of the occurrence.

The compensating detection control that is used to look for these types of transactions, the Taxpayer Account Maintenance Activity Report, is not utilized by management. Policies, especially those without effective monitoring for violations, can not prevent alteration of accounts.

Currently, the GENTS system has the ability to restrict employees from looking at certain accounts, called restricted accounts. A select few employees are given the ability to access these accounts.

Recommendation

We recommend that the division create an indicator to be placed on the system that would alert management when a user makes an adjustment to
their own account. In addition, these adjustments should be reviewed by upper management to ensure compliance with the existing policy.

Database Administration

A review of the security and controls over the Oracle and SQL databases noted that the majority of controls and security measures in place are adequate to protect the data from unauthorized access or use. We did note, however, that some areas should be strengthened in order to provide better control. Details of these specific control improvements have been communicated in our management letter.

Field Auditor Laptops

A review of the security over confidential taxpayer data stored on field auditor laptop computers was performed to determine whether controls are in place to protect it from unauthorized access, viewing and use. We noted that sensitive taxpayer data is not encrypted. The division currently does not have a policy in place requiring the encryption of sensitive data stored on these laptop computers. An industry best practice states that a policy on the use of cryptographic controls for protection of information should be developed and implemented. It should include, among other things, the use of encryption for protection of sensitive information transported by mobile or removable media, devices or across communication lines. In the absence of encryption, a laptop that is lost or stolen may have the information stored on it inappropriately disclosed or misused.

Recommendation

The division is currently reviewing an encryption strategy for use on their laptop computers. They
expect to have this completed and rolled out by August 2007. We recommend that the division continue their efforts in pursuing an encryption strategy and have it in place as soon as possible.

Documentation

Of the 15 online filing applications other than NJWebfile, 11 had no application documentation and the remaining four applications had inadequate documentation. This condition was also noted in a prior report dated December 11, 2002. Since then, the division and OIT have not created documentation for the online filing applications other than NJWebfile, which was created by an outside vendor that works with the division staff to provide and update the documentation regularly.

Detailed system documentation should be developed during the acquisition and maintenance process for all applications. As the experienced developers and programmers who are essential to these programs leave service, the lack of documentation will create issues if the processes, platforms, or programs involved in these applications require change. The additional time and resources that will be needed at that time will be greater than the time spent documenting the system currently.

Recommendation

We recommend that the division work with OIT to develop documentation for all online filing applications. This documentation should include, at a minimum, information about the flow of data through the program, descriptions of all data edits and calculations in the application, and a detailed error handling process.
Physical Access

Based on our conversations with the division’s employees responsible for physical security of the Taxation building computer room, we determined that the combination on the cipher entry lock has not been changed in approximately three years. Between June 2006 and June 2007 one employee on the access list retired and one was suspended, but the code still has not been changed. The division’s policy states that the code is to be changed when a staff member is terminated or resigns. Turnover in this area is not common, and most employees leave on good terms, so the division does not see the need to change the code.

Failure to change the code on a regular basis, both at specific events and at regular intervals, could lead to many users having physical access to the NJWebfile database machines. This could lead to compromise or destruction of the machines or data. Also, the person charged with oversight of access to this area should be aware of all users with access and should have a comprehensive access control list.

Recommendation

We recommend that the cipher lock code be changed as soon as possible, and the existing policy be adjusted to include changing the code when an employee leaves service for any reason as well as more frequent periodic changes. Also, once the code is changed a comprehensive access control list should be created, maintained, and adhered to at all times.
Mr. Richard L. Fair  
State Auditor  
Office of Legislative Services  
125 South Warren Street  
P. O. Box 067  
Trenton NJ 08625-0067

Dear Mr. Fair:

This is in response to the draft audit report regarding the Division of Taxation's Online Database Security. I have reviewed the report and offer the following comments:

1) **System Administration Recommendation:**

   We recommend management provide adequate resources to effectively administer the servers, finalize and implement draft policies to provide measurable standards for effectively mitigating potential security risks, and periodically review files, directories and security configurations to protect against unauthorized access or compromise.

This finding and recommendation fall within the purview of the Office of Information Technology (OIT). The OIT management response follows:

OIT management has taken a number of proactive steps to addressing the OLS audit finding recommendations regarding the risk of unauthorized access or compromise. This past year OIT created the Statewide Information Security Office and has been working towards building out the resources in the office. Recently one additional staff was hired and a second is in process. This Office will place significant emphasis on developing the necessary statewide policies for which the audit raised concerns. As well this Office will develop an awareness and training program to disseminate these polices to all agencies and publish statewide standards in this same regard.

To continue to address this effort this Office has adopted the ISO 17799 security policy framework as a model for the enterprise security policy program. To date 13 policies have been drafted and adopted with several others under development. OIT management remains committed to the
furtherment of statewide security and will continue to place the appropriate emphasis on this Office.

We welcome future audits to continually monitor our progress and look forward to your recommendations.

2) **Gents Access Recommendations:**

**Comprehensive review of GENTS access**

*We recommend that the division initiate a comprehensive review of GENTS access statewide. It should include reviewing access needs and roles with the users of the system from the bottom up, reviewing existing profiles in GENTS for relevance, and creating or adjusting roles in GENTS as necessary. In addition, access for each employee should be reviewed to determine if it is appropriate and necessary in this revised structure.*

Employee access information for all Division employees can be provided to each of the respective senior managers for their review to determine each individual’s appropriate level of authority or necessary access. A reasonable beginning step may be to provide TAXNET inquiry-only menus for the 897 Division employees identified in the audit as not having made an update in the audit period. Additional TAXNET conversations and access rights can then be provided on a case-by-case basis as appropriate.

**Creation of restricted account for all employees**

*We recommend that the division create an additional set of restricted accounts that includes all employees with access to change accounts in GENTS. The current DEROs could be given the ability to work on these accounts as well as upper management. Transactions could be approved as before, but this would eliminate the majority of employees being able to view or change their own account. In addition, the division could create a review system for all transactions adjusted by DEROs and upper management to ensure compliance with the existing policy.*

The Division will meet with OIT to explore the feasibility of restricting access by employees to their own tax accounts based on the employee’s logon-id. Alternatively we will explore identifying employees that access their own accounts through a system report. By creating an additional set of restricted accounts for Division employees with GENTS access, all refunds/rebates and bills for these employees will require manual review and approval. This is in addition to any adjustments that may be required. During peak income tax and rebate processing seasons, the current
resources within the Division of Taxation would not be adequate to administer these accounts timely. In any case, the social security numbers of all employees and their spouses will need to be maintained by the Division.

3) **Field Auditor Laptops Recommendation:**

*The division is currently reviewing an encryption strategy for use on their laptop computers. They expect to have this completed and rolled out by August 2007. We recommend that the division continue their efforts in pursuing an encryption strategy and have it in place as soon as possible.*

As noted in the recommendation, the Division is in the process of implementing an encryption strategy for use on laptop computers.

4) **Documentation Recommendation:**

*We recommend that the division ensure that adequate documentation exists for all online filing applications. This documentation should include, at a minimum, information about the flow of data through the program, descriptions of all data edits and calculations in the application, and a detailed error handling process.*

The need for adequate documentation is duly noted and the Division will review the system documentation recommendation with OIT management. However, the need to implement legislative mandates, revenue initiatives and other priorities in timely manner must continue to take precedence. The Division of Taxation will continue to assess this recommendation as priorities shift.

5) **Physical Access Recommendation**

*We recommend that the cipher lock code be changed as soon as possible, and the existing policy be adjusted to include changing the code when an employee leaves service for any reason as well as more frequent periodic changes. Also, once the code is changed a comprehensive access control list should be created, maintained, and adhered to at all times.*

The cipher entry lock on the eighth floor data room door has been changed and the comprehensive access list has been updated. The cipher lock code will be changed on a regular basis and at specific events in accordance with the audit recommendations.
With regard to Database Administration, the Division of Taxation will work with OIT to implement the suggested access changes to the Oracle database at OIT. The recommended actions with regard to the SQL database have been implemented and the suggested reviews will be done periodically.

If you have any questions regarding the above, please do not hesitate to contact me. Thank you for this opportunity to respond.

Sincerely,

[Signature]

Maureen Adams
Acting Director
Division of Taxation